

United States Court of Appeals for  
the District of Columbia Circuit

---

**No. 24-1113**

(and Consolidated Cases Nos. 24-1130 & 24-1183)

---

TIKTOK INC. and BYTEDANCE LTD.,

*Petitioners,*

v.

MERRICK B. GARLAND, in his official capacity as  
Attorney General of the United States,

*Respondent.*

(Caption Continued on Inside Cover)

On Petition for Review of the Protecting Americans from  
Foreign Adversary Controlled Applications Act

---

---

**BRIEF OF *AMICUS CURIAE* THE FOUNDATION FOR DEFENSE  
OF DEMOCRACIES IN SUPPORT OF RESPONDENT**

---

Peter C. Choharis  
Arnon D. Siegel  
The Choharis Law Group, PLLC  
1300 19th Street, NW, Suite 620  
Washington, DC 20036  
(202) 587-4478  
peter@choharislaw.com  
*Counsel for Amicus Curiae*

August 2, 2024

---

BRIAN FIREBAUGH, *et al.*,

*Petitioners,*

v.

MERRICK B. GARLAND, in his official capacity as  
Attorney General of the United States,

*Respondent.*

BASED POLITICS INC.,

*Petitioner,*

v.

MERRICK B. GARLAND, in his official capacity as  
Attorney General of the United States,

*Respondent.*

---

### **CIRCUIT RULE 29(D) STATEMENT**

Amicus Curiae the Foundation for Defense of Democracies (“FDD”) certifies that it is not aware of any other amicus brief addressing the subject of this brief, specifically the grave national security threats that TikTok and ByteDance pose to our nation. A separate brief is therefore necessary to permit FDD to offer its perspectives on the issues before the Court.

All parties have consented to the filing of this brief.

### **CERTIFICATE AS TO PARTIES, RULINGS, AND RELATED CASES**

- A. *Parties and Amici.* Except for the Amicus Curiae filing this brief, all parties, intervenors, and amici appearing before this Court of which Amicus is aware are listed in the Briefs for Petitioner and Respondent.
- B. *Rulings Under Review.* An accurate reference to the law at issue appears in the Briefs for Petitioner and Respondent.
- C. *Related Cases.* Counsel for Amicus Curiae are not aware of any other case currently pending before this or any other court that is related to this case within the meaning of this Court’s Rule 28(a)(1)(C).

**CORPORATE DISCLOSURE STATEMENT**

Pursuant to Federal Rule of Appellate Procedure 26.1 and this Court’s Rule 26.1, FDD states that it has no parent corporations and that no publicly held entity owns ten percent (10%) or more of it.

**STATEMENT OF AUTHORSHIP AND  
FINANCIAL CONTRIBUTIONS**

Amicus Curiae FDD certifies that no party or party’s counsel authored this brief in whole or in any part; that no party or party’s counsel provided any money intended to fund the preparation or submission of this brief; and that no party or person, other than Amicus, or Amicus’s counsel, contributed money intended to fund the preparation or submission of this brief.

**INTEREST OF THE AMICUS CURIAE**

The Foundation for Defense of Democracies (FDD) is a nonpartisan 501(c)(3) research institute based in Washington, D.C., and focusing on national security and foreign policy. FDD conducts in-depth research, produces accurate and timely analyses, identifies illicit activities, and provides policy options – all with the aim of strengthening the national security of the United States and reducing or eliminating threats posed by adversaries and enemies of the United States and other free nations. FDD does not accept donations from any foreign governments. For more information, visit [www.fdd.org](http://www.fdd.org).

## TABLE OF CONTENTS

CIRCUIT RULE 29(D) STATEMENT .....	i
CERTIFICATE AS TO PARTIES, RULINGS, AND RELATED CASES .....	i
CORPORATE DISCLOSURE STATEMENT .....	ii
STATEMENT OF AUTHORSHIP AND FINANCIAL CONTRIBUTIONS .....	ii
INTEREST OF THE AMICUS CURIAE .....	ii
TABLE OF CONTENTS.....	iii
TABLE OF AUTHORITIES .....	iv
BACKGROUND .....	1
SUMMARY OF ARGUMENT.....	9
ARGUMENT .....	9
I.          TIKTOK POSES THREATS TO U.S. NATIONAL SECURITY.....	9
A.      TikTok Has Conducted U.S. Surveillance and Shared Its Results With Beijing.....	10
B.      TikTok Enables the PRC to Interfere With U.S. Elections, Manipulate Information That Is Sensitive to China, and Conduct Psychological Warfare. ....	15
CONCLUSION.....	25
CERTIFICATE OF COMPLIANCE .....	27
CERTIFICATE OF SERVICE .....	28

## TABLE OF AUTHORITIES

### CASES

<i>Boumediene v. Bush</i> , 553 U.S. 723 (2008).....	31
<i>China Telecom (Ams.) Corp. v. FCC</i> , 57 F.4th 256 (D.C. Cir. 2022).....	31
<i>Terminiello v. City of Chicago</i> , 337 U.S. 1, (1949).....	34
<i>Trump v. Hawaii</i> , 585 U.S. (2018) .....	31

### OTHER AUTHORITIES

“An Overview of Deepfake: The Sword of Damocles in AI 265,” 2020 International Conference on Computer Vision, Image and Deep Learning, CVIDL (July 10, 2020).....	17
“The Secretary of the Patriotic Party Said Wildly to Cut Off the Heads of Netizens, and an Office Photo Betrayed Him” APOLLO NEWS (July 17, 2012).....	14
Bradley Bowman, ed., “Cognitive Combat China, Russia, and Iran’s Information War Against Americans,” FOUND. DEF. DEMOC., at 8-9 & nn. 9-18 (June 2024) (“FDD Monographs”).....	27
Brian Fung, “Analysis: There is Now Some Public Evidence that China Viewed TikTok Data,” CNN BUSINESS (June 8, 2023).....	24
China Defence Universities Tracker, “Huazhong University of Science and Technology” Australian Strategic Policy Institute & International Cyber Policy Centre, available at <a href="https://unitracker.aspi.org.au/universities/huazhong-university-of-science-and-technology/">https://unitracker.aspi.org.au/universities/huazhong-university-of-science-and-technology/</a> .....	17
China Law Translate, “Data Security Law of the PRC” (June 10, 2021).....	12
China Law Translate, “National Security Law,” (Jul. 1, 2015) .....	11
China Law Translate, “People’s Republic of China Counter-Espionage Law (2023 Edition)” (Apr. 26, 2023).....	12
China Law Translate, “PRC National Intelligence Law (as amended in 2018)” (June 27, 2017).....	12
Claire Fu, Daisuke Wakabayashi, “There Is No TikTok in China, but There Is Douyin. Here’s What It Is,” <i>NEW YORK TIMES</i> , (Apr. 25, 2024).....	18
Craig Singleton, “China,” published in FDD Monographs, <i>supra</i> n.59 at 14 (June 2022).....	28
Dan Goodin, “TikTok and 32 other iOS Apps Still Snoop Your Sensitive Clipboard Data,” <i>ARS TECHNICA</i> (June 27, 2020).....	22
Emily Baker-White, “LinkedIn Profiles Indicate 300 Current TikTok and ByteDance Employees Used to Work for Chinese State Media—And Some Still Do,” <i>FORBES</i> (Aug. 11, 2022).....	16
FDD Report <i>supra</i> n.12 .....	13
Foundation for Defense of Democracies, “5 Things to know about Bytedance,	

TikTok’s Parent Company” (Mar. 12, 2024) .....	13
Gaute Friis, Nickson Quak, Sara Shah, and Elliot Stewart, “Countering China’s Use of Private Firms in Covert Information Operations” STANFORD FREEMAN SPOGLI INSTITUTE FOR INTERNATIONAL STUDIES, at 5 (June 21, 2024) .....	20
Georgia Wells and Byron Tau, “TikTok Tracked Users Who Watched Gay Content, Prompting Employee Complaints,” WALL ST. J. (May 5, 2023).....	22
Georgia Wells and Sadie Gurman, “TikTok Collected U.S. Users’ Views on Gun Control, Abortion and Religion, U.S. Says,” WALL STREET JOURNAL (July 27, 2024) .....	23
He Jian, “The List of Party Branches is Exposed, Where is Douyin Going” EPOCH TIMES (Aug. 5, 2020).....	16
John Fitzgerald, “Beijing’s Quoqing Versus Australia’s way of life”, (Sep. 27, 2016) available at:.....	10
Juro Osawa, Amir Efrati, and Shai Oster, “TikTok Still Has Key Software Developers in China Despite Effort to Move Offshore,” THE INFORMATION (Aug. 26, 2021) .....	16
Law Info China, “Cybersecurity Law of the People’s Republic of China,” (Nov. 7, 2016),.....	12
Li Yuan, “China’s TikTok Blaze New Ground That Could Doom It,” NEW YORK TIMES (Nov. 5, 2019).....	14
Nathan Beauchamp-Mustafaga, “Chinese Next-Generation Psychological Warfare,” RAND at iv-v (June 1, 2023) .....	28
National Intelligence Council, “Intelligence Community Assessment, Foreign Threats to the 2022 U.S. Elections,” ICA 2022-27259-A, at p. i (Dec. 23, 2022) 21, 25	
Network Contagion Research Institute (NCRI) and Miller Center on Policing and Community Resilience of Rutgers University, “A Tik-Tok-ing Timebomb: How TikTok's Global Platform Anomalies Align with the Chinese Communist Party's Geostrategic Objectives" (Dec. 2023) .....	25
Nita Farahany, “TikTok is part of China’s cognitive warfare Campaign,” Opinion, GUARDIAN, (Mar. 25, 2023) .....	29
Office of the Director of National Intelligence, “Annual Threat Assessment of the U.S. Intelligence Community,” at 12 (Feb. 5, 2024) (“Annual Threat Assessment”) .....	21
Petitioner’s Br., Doc. #2060743, at 50 .....	18
Ryan McMorrow, Qianer Liu and Cheng Leng, “China Moves to Take ‘Golden Shares’ in Alibaba and Tencent Units,” FINANCIAL TIMES (Jan. 12, 2023).....	13
Sapna Maheshwari and Ryan Mac, “Driver’s Licenses, Addresses, Photos: Inside How TikTok Shares User Data,” NEW YORK TIMES (May 24, 2023).....	23
Senate Select Committee on Foreign Interference through Social Media,” (Mar. 14, 2023)” [hereafter, “Australian Report”] .....	10
Stipulated Order for Civil Penalties, Permanent Injunction, and Other Relief, Case	

No. 2:19-cv-1439, <i>United States v. Music.ly</i> , No. 2:19-1439 (C.D. Cal.) .....	23
TikTok Brief, Doc. # 2060743, at 14, 50-58 .....	30
TikTok Petition for Review ¶ 16. ....	17
TikTok, “Covert Influence Operations” (2024) available at .....	21
TikTok, “Labelling State-Affiliated Media Entities” (2024) .....	22
Transcript, Hon. Christopher Wray, “2022 Josh Rosenthal Memorial Talk,” GERALD R. FORD SCHOOL OF PUBLIC POLICY, U. MICH. (Dec. 2, 2022) .....	19
US House Committee on Energy and Commerce, Testimony of Shou Chew Chief Executive Officer, TikTok Inc. (Mar. 23, 2023) at 6 .....	13
Xinhua News Agency, “Decision of the Central Committee of the Communist Party of China on Several Major Issues Concerning Comprehensively Deepening Reform,” (Nov. 2013) available at: <a href="https://archive.ph/hs5gH#selection-507.0-507.133">https://archive.ph/hs5gH#selection-507.0- 507.133</a> .....	11
Yingzhi Yang and Bhargav Acharya, “ByteDance Founder Zhang Yiming Steps Down as Chairman,” REUTERS (Nov. 3, 2021) .....	15
Yuan Yang and James Fontanella-Khan, “Grindr Is Being Sold by Chinese Owner After U.S. Raises National Security Concerns,” L.A. TIMES (Mar. 6, 2020) .....	32



## BACKGROUND

For decades, the Chinese Communist Party (“CCP” or “Party”) has required that the internet, and later web-based companies and their Apps, be controlled and then exploited in service of the Party and the domestic and international interests of the People’s Republic of China’s (“PRC”).<sup>1</sup> In September 2004, the CCP passed its “Decision on Enhancing the Party’s Governance Capability,” “which formally designated the internet as a domain for Party control and influence: ‘Attach great importance to the influence of new types of media channels, such as the internet, on public opinion. . . . Strengthen the construction of internet propaganda teams and form a strong online positive public opinion.’”<sup>2</sup> In November 2013, the Party introduced the “Decision on ‘Some Major Issues Concerning Comprehensively Deepening Reform,’” which declared: “We will straighten out the mechanism for both domestic and overseas propaganda and support key media groups to develop both at home and

---

<sup>1</sup> Much of this background is based on the report by Rachel Lee, Prudence Luttrell, Matthew Johnson, and John Garnaut, “TikTok, ByteDance, and Their ties to the Chinese Communist Party, Submission [No. 34] to the [Australian] Senate Select Committee on Foreign Interference through Social Media” (Mar. 14, 2023) (the “Australian Report”), available at

<https://www.scribd.com/document/633015202/TikTok-ByteDance-And-Their-Tis-to-the-Chinese-Communist-Party>

The Australian Report presents a detailed account by the PRC and its intelligence and military assets of the use of social media platforms, especially TikTok and ByteDance, to promote the PRC’s (and CCP’s) domestic and foreign interests.”

<sup>2</sup> *Id.* at 17; see John Fitzgerald, “Beijing’s Quoqing Versus Australia’s Way of Life” (Sep. 27, 2016), available at

<https://insidestory.org.au/beijings-guoqing-versus-australias-way-of-life/>

abroad. We will foster external-facing cultural enterprises and support cultural enterprises to go abroad and expand markets there.”<sup>3</sup> In August 2021, the PRC’s state news agency, Xinhua, confirmed that TikTok was an integral part of the PRC’s “domestic and overseas propaganda.”<sup>4</sup> Xinhua explained that “Various short video apps represented by TikTok have emerged” as “platforms to become ‘megaphones’ for ‘telling the China story well and spreading Chinese voices well.’”<sup>5</sup>

Having identified video apps generally, and TikTok specifically, as means to promote CCP propaganda, the PRC enacted laws and practices that ensured both *de jure* and *de facto* control over these companies to serve the PRC and preserve the CCP’s power and influence.

#### *The PRC’s Legal Control over ByteDance and TikTok*

In 2015, the PRC passed the National Security Law, which among other things “requires citizens and organizations to report acts harming national security and to support national security bodies, public security bodies, and military bodies in their work.”<sup>6</sup> China’s National Intelligence Law of 2017 obligates all Chinese organizations

---

<sup>3</sup> China Law Translate, “National Security Law,” (July 1, 2015), available at: <https://www.chinalawtranslate.com/2015nsl/>.

<sup>4</sup> Xinhua News Agency, “Decision of the Central Committee of the Communist Party of China on Several Major Issues Concerning Comprehensively Deepening Reform,” (Nov. 2013) available at: <https://archive.ph/hs5gH#selection-507.0-507.133>.

<sup>5</sup> *Id.*

<sup>6</sup> China Law Translate, “National Security Law,” (July 1, 2015), available at <https://www.chinalawtranslate.com/2015nsl/>

and citizens to collaborate with state intelligence operations.<sup>7</sup> That means that all persons and organizations must “support China’s intelligence services by secretly turning over data collected in China or overseas.”<sup>8</sup> Also, in 2017, the PRC passed the National Cybersecurity Law, which “compels companies and individuals to make networks, data, and communications available to the police and security services.”<sup>9</sup> The Data Security Law of 2021 gives the PRC authority “to access and control private data, including China’s “national” data processed overseas.”<sup>10</sup> China’s recently revised Counter-Espionage Law of 2023 bolsters the state’s authority, making clear that all technological developments, whether designed for civilian or for military use, must be available to state security and intelligence services.<sup>11</sup>

The cumulative effect of these laws is to require companies and their innovations, such as ByteDance and its TikTok app, to serve the Chinese state as much or more than to serve their customers. But the PRC’s state authorities do not rely on law alone to achieve their ends. As it had with many other companies, the PRC

---

<sup>7</sup> China Law Translate, “PRC National Intelligence Law (as amended in 2018)” (June 27, 2017) available at <https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/>.

<sup>8</sup> The Australian Report, *supra* n.1, at 22 (citation omitted).

<sup>9</sup> Law Info China, “Cybersecurity Law of the People’s Republic of China,” (Nov. 7, 2016), available at <https://www.lawinfochina.com/Display.aspx?Id=22826&Lib=law&LookType=3>.

<sup>10</sup> China Law Translate, “Data Security Law of the PRC” (June 10, 2021), available at <https://www.chinalawtranslate.com/en/datasecuritylaw/>.

<sup>11</sup> China Law Translate, “People’s Republic of China Counter-Espionage Law (2023 Edition)” (Apr. 26, 2023), available at <https://www.chinalawtranslate.com/counter-espionage-law-2023/>.

assumed control over ByteDance, as well as TikTok and its Chinese sister company,

Douyin, by controlling management and infiltrating ByteDance with CCP personnel.

*The PRC and CCP's Infiltration of TikTok's Parent, ByteDance*

In April 2021, a Cyberspace Administration of China (“CAC”)-connected fund, along with two other PRC agencies, acquired a one percent (1%) stake in Petitioner ByteDance’s primary Chinese subsidiary, Beijing ByteDance Technology Co., Ltd. (“Beijing ByteDance,” renamed “Douyin”).<sup>12</sup> While TikTok likes to say that it is almost entirely owned by private parties, including U.S. private equity firms,<sup>13</sup> what it does not disclose is how the Chinese government uses its small ownership share, called a “golden share,” to exercise control over Chinese companies.<sup>14</sup> For example, the one-percent equity stake held by CAC and other agencies gives the Chinese government the power to appoint one of Beijing ByteDance/Douyin’s three members of the Board of Directors.<sup>15</sup> The Director chosen by CAC was Wu Shugang, the Party secretary of the Communist Youth League under the Ministry of Education. Wu gained notoriety

---

<sup>12</sup> See Foundation for Defense of Democracies, “5 Things to know about Bytedance, TikTok’s Parent Company” (Mar. 12, 2024), available at <https://www.fdd.org/analysis/2024/03/12/5-things-to-know-about-bytedance-tiktoks-parent-company>; Australian Report at 44. See generally Australian Report at 43-48, 32-39; 25-30.

<sup>13</sup> See US House Committee on Energy and Commerce, Testimony of Shou Chew Chief Executive Officer, TikTok Inc. (Mar. 23, 2023) at 6, available at [https://d1dth6e84htgma.cloudfront.net/Written\\_Testimony\\_of\\_Shou\\_Chew\\_c07504eccf\\_084e8683f3.pdf?updated\\_at=2023-03-22T03:10:22.760Z](https://d1dth6e84htgma.cloudfront.net/Written_Testimony_of_Shou_Chew_c07504eccf_084e8683f3.pdf?updated_at=2023-03-22T03:10:22.760Z)

<sup>14</sup> See Ryan McMorro, Qianer Liu and Cheng Leng, “China Moves to Take ‘Golden Shares’ in Alibaba and Tencent Units,” FINANCIAL TIMES (Jan. 12, 2023), available at <https://archive.md/PmxYE>.

<sup>15</sup> See FDD Report *supra* n.12, at 12; Australian Report, *supra* n.1, at 44-45.

in 2012, when he posted, “I only have one wish – that one day I can cut off the dog head of traitors. Let the Chinese traitors preaching so-called ‘human rights and freedom’ go to hell!!”<sup>16</sup> Wu’s authority at Beijing ByteDance included the “power to control the content at ByteDance’s media platforms in China” and “the right to appoint the group’s chief censor, known at Chinese internet groups as the ‘editor in chief.’”<sup>17</sup>

As a result, the CCP exercises strategic control over ByteDance and its subsidiaries, TikTok and China-focused Douyin. The CCP’s control is not focused on commercial matters the way a board member of Western private company would focus. Rather, the Party’s “golden share” allows it to focus on the Party’s and Chinese government’s strategic goals domestically (in the case of Douyin) and overseas (in the case of TikTok).<sup>18</sup> As set forth in Section I *infra*, these interests include both accessing overseas data about individuals and targeting individuals or groups of individuals for pro-PRC messaging campaigns.

But while China’s legal requirements and its ByteDance board seat have allowed Chinese authorities to gain access to ByteDance’s (and likely TikTok’s) strategic objectives, the CCP’s greatest power and influence over these companies

---

<sup>16</sup> “The Secretary of the Patriotic Party Said Wildly to Cut Off the Heads of Netizens, and an Office Photo Betrayed Him,” APOLLO NEWS (July 17, 2012), available at <https://archive.md/yGthO>.

<sup>17</sup> *See supra*, n. 14.

<sup>18</sup> Li Yuan, “China’s TikTok Blaze New Ground That Could Doom It,” N. Y. TIMES (Nov. 5, 2019), available at <https://web.archive.org/web/20220930033958/https://www.nytimes.com/2019/11/05/business/tiktok-china-bytedance.html>.

stem from the Party's practice of infiltrating Chinese technology companies, including ByteDance, with Party members who create "cells" within the companies. "The divide between private and public companies in China has narrowed in recent years through the Party's aggressive expansion of Party organizations within private firms and its use of extra-legal measures to purge prominent leaders within those firms."<sup>19</sup> The removal of Jack Ma, Alibaba's founder, from the company's senior management is perhaps the best known example of this trend.<sup>20</sup>

The CCP "operates party cells throughout ByteDance's hierarchy, affording it direct access to ByteDance's technology and strategic insights" and goals.<sup>21</sup> These "Party structures are not designed to be visible or accountable to international regulators, partners, investors, or consumers"—or U.S. courts—making the extent of its power and influence difficult to estimate or even document.<sup>22</sup> But there is no question that ByteDance exercises enormous control over TikTok irrespective of the legal formalities of the companies' corporate structures.<sup>23</sup> And *Forbes* has reported

---

<sup>19</sup> Australian Report, *supra* n.1, at 32.

<sup>20</sup> Not surprisingly, as were the Founder-CEOs of Alibaba and Pinduoduo, ByteDance Founder and CEO Zhang Yiming was also forced to resign in November 2021. See Yingzhi Yang and Bhargav Acharya, "ByteDance Founder Zhang Yiming Steps Down as Chairman," REUTERS (Nov. 3, 2021), available at <https://www.reuters.com/article/bytedance-reshuffling-1103-wedn-idCNKBS2HO06L>.

<sup>21</sup> Foundation for Defense of Democracies, "5 Things to know about Bytedance, TikTok's Parent Company," *supra* n. 12.

<sup>22</sup> Australian Report, *supra* n.1, at 33.

<sup>23</sup> See *id.* at 40-45; see also *supra* n. 21; Juro Osawa, Amir Efrati, and Shai Oster, "TikTok Still Has Key Software Developers in China Despite Effort to Move Offshore," THE INFORMATION (Aug. 26, 2021), available at

that “[t]hree hundred current employees at TikTok and ByteDance previously worked for Chinese state media publications,” and that fifty of the “employees [] work for or on TikTok, including a content strategy manager who was formerly a Chief Correspondent for Xinhua News,” which the U.S. State Department deems “a foreign government functionary.”<sup>24</sup> In fact, fifteen ByteDance employees were also employed *at the same time* by Xinhua and other Chinese state media entities, all foreign government functionaries.<sup>25</sup>

Perhaps this explains ByteDance’s close connection to China’s military and intelligence services. For example, in 2018, ByteDance established the Beijing Academy of Artificial Intelligence at the behest of China’s Ministry of Science and Technology.<sup>26</sup> This nominally academic institution uses civilian development of AI technology for military applications, including the promotion of AI in the field of “national defense innovation.”<sup>27</sup>

ByteDance’s military ties extend to other high-risk defense institutions with links to China’s People’s Liberation Army. For instance, ByteDance researchers have

---

<https://www.theinformation.com/articles/tiktok-still-has-key-software-developers-in-china-despite-effort-to-move-offshore>.

<sup>24</sup> Emily Baker-White, “LinkedIn Profiles Indicate 300 Current TikTok and ByteDance Employees Used to Work for Chinese State Media—And Some Still Do,” FORBES (Aug. 11, 2022), available at <https://www.forbes.com/sites/emilybaker-white/2022/08/10/bytedance-tiktok-china-state-media-propaganda/>.

<sup>25</sup> *Id.*

<sup>26</sup> FDD Report, *supra* n.12.

<sup>27</sup> *Id.*

collaborated on cutting-edge AI research with scientists from the Huazhong University of Science and Technology, which hosts a large number of PRC government-funded and directed defense laboratories working on projects involving, among other things, the development artificial intelligence and imaging technology for weapons.<sup>28</sup> ByteDance researchers have also worked on developing deepfakes, a type of AI that can spread misinformation and disinformation, with individuals from the People's Public Security University of China, which is involved in developing technological tools for China's repressive public security apparatus, including its Ministry of Public Security.<sup>29</sup>

Finally, we observe that TikTok/ByteDance's Petition coyly reveals to this Court that "TikTok is not offered in the People's Republic of China."<sup>30</sup> Instead, its sister company, Douyin, operates in China. Why? Why would TikTok, an extraordinarily successful Chinese-controlled company with a global reach, not be "offered" in China—especially when there is so much overlap of TikTok and Douyin's

---

<sup>28</sup> See China Defence Universities Tracker, "Huazhong University of Science and Technology" Australian Strategic Policy Institute & International Cyber Policy Centre, available at

<https://unitracker.aspi.org.au/universities/huazhong-university-of-science-and-technology/>.

<sup>29</sup> See "An Overview of Deepfake: The Sword of Damocles in AI 265," 2020 International Conference on Computer Vision, Image and Deep Learning, CVIDL (July 10, 2020) available at <https://archive.ph/VPnsN>; see also China Defence Universities Tracker, "People's Public Security University of China," Australian Strategic Policy Institute & International Cyber Policy Centre, available at <https://unitracker.aspi.org.au/universities/peoples-public-security-university-of-china/>.

<sup>30</sup> TikTok Petition for Review ¶ 16.



leadership and resources?<sup>31</sup> As is typical of ByteDance and its subsidiaries, the reasons for the companies' decisions are not public. But one compelling business need would be to distance TikTok from the PRC's use of Douyin for extensive domestic surveillance and AI technology to monitor and suppress dissent, which would expose TikTok to sanctions by the U.S. and other western governments.<sup>32</sup>

## SUMMARY OF ARGUMENT

TikTok, one of the world's most popular social media apps, is a tool of the Chinese Communist Party. The CCP uses TikTok to serve certain of the interests of the People's Republic of China. Those interests are contrary to the national security interests of the United States – and TikTok and its parent, ByteDance, thus pose serious threats to America. In requiring that ByteDance divest itself of TikTok, Congress has implemented measures to protect American national security interests. Those measures are not simply wise, but constitutional.

## ARGUMENT

### I. TIKTOK POSES THREATS TO U.S. NATIONAL SECURITY.

Petitioners TikTok/ByteDance says that this case is about “speech[] content,” because the House Committee Report complains about “misinformation,

---

<sup>31</sup> See Australian Report, *supra* n.1, at 39, 43. See generally *id.* at 39-44.

<sup>32</sup> See FDD Report, *supra* n. 12; Claire Fu, Daisuke Wakabayashi, “There Is No TikTok in China, but There Is Douyin. Here’s What It Is,” N. Y. TIMES (Apr. 25, 2024) available at <https://www.nytimes.com/2024/04/25/business/china-tiktok-douyin.html>.

disinformation, and propaganda.”<sup>33</sup> But the threat understood by the Congress and the President when passing the Protecting Americans from Foreign Adversary Controlled Applications Act, Pub. L. No. 118-50, div. H, 138 Stat. 955 (2024) (the “Act”), is far greater than the transmission of information or even disinformation.

[T]he concern is not just that an app with TikTok’s data harvesting and targeted recommendation capabilities could be used as a platform for disseminating propaganda, disinformation, and other messages designed to influence democratic societies. Rather, it is that TikTok has the potential to sway elections, corrode people’s faith in democracy, and undermine the will of open societies to compete against China’s authoritarian model globally.<sup>34</sup>

In fact, these concerns are not hypothetical, despite what TikTok/ByteDance would have this Court believe.<sup>35</sup> Rather, even the *public* evidence to which the House and Senate had ready access shows that TikTok/ByteDance has already engaged in conduct that has threatened U.S. national security and can do so on a much greater scale should the PRC so decide.

**A. TikTok Has Conducted U.S. Surveillance and Shared Its Results With Beijing.**

Speaking at the University of Michigan in December 2022, FBI Director Christopher Wray identified three threats posed by TikTok and its parent ByteDance: “One, it gives them the ability to control the recommendation algorithm, which allows them to manipulate content and if they want to, to use it for influence operations which

---

<sup>33</sup> Petitioner’s Br., Doc. #2060743, at 50.

<sup>34</sup> Australian Report, *supra* n. 1 at 24.

<sup>35</sup> *See id.* at 50-54.

are a lot more worrisome in the hands of the Chinese Communist Party.”<sup>36</sup> Second, TikTok/ByteDance has “the ability to collect data through it on users which can be used for traditional espionage operations.”<sup>37</sup> And third, TikTok/ByteDance has “access to the software . . . millions of [users’] devices and that gives them the ability to engage in different kinds of malicious cyber activity.”<sup>38</sup> Director Wray made clear that “all of these things are in the hands of a [PRC] government that doesn’t share our values and that has a mission that’s very much at odds with what’s in the best interest of the United States.”<sup>39</sup>

Director Wray’s concerns were not hypothetical: They were based on experience. For example, regarding Wray’s first point, national security analysts have developed the concept of foreign information manipulation and interference (“FIMI”) to describe foreign state and non-state actors, and privatized FIMI (“PFIMI”) to describe commercial actors, who spread disinformation and manipulate populations. While the most famous FIMI was Russia’s interference in the 2016 U.S. presidential election, the PRC’s attempts at FIMI were crude and ineffective, according to a very

---

<sup>36</sup> Transcript, Hon. Christopher Wray, “2022 Josh Rosenthal Memorial Talk,” GERALD R. FORD SCHOOL OF PUBLIC POLICY, U. MICH. (Dec. 2, 2022), available at <https://fordschool.umich.edu/video/2022/christopher-wray-2022-josh-rosenthal-memorial-talk>.

<sup>37</sup> *Id.*

<sup>38</sup> *Id.*

<sup>39</sup> *Id.*

recent Stanford study.<sup>40</sup> Instead, by “tapping into a pool of private talent and innovation that has developed in the digital marketing and social media influence industries, the PRC is bolstering its ability to disseminate its narratives and manipulate public discourse on a global scale.”<sup>41</sup> The empirical study acknowledged that it had only “a partial glimpse” into the “clandestine” system run by the PRC, yet still was able to determine that “covert FIMI in the PRC is an industrial-scale endeavor involving dozens of actors at all levels of society. It involves both national and local governments, the military, the media and the propaganda system, China’s intelligence and security services, commercial enterprises, and even organized crime groups.”<sup>42</sup>

Director Wray’s comments reflect the consensus view of the U.S. intelligence community. This year’s Annual Threat Assessment said that “China is demonstrating a higher degree of sophistication in its influence activity, including experimenting with generative AI.”<sup>43</sup> “Beijing is intensifying efforts to mold U.S. public discourse,” the

---

<sup>40</sup> Gaute Friis, Nickson Quak, Sara Shah, and Elliot Stewart, “Countering China’s Use of Private Firms in Covert Information Operations” STANFORD FREEMAN SPOGLI INSTITUTE FOR INTERNATIONAL STUDIES, at 5 (June 21, 2024) available at

[https://stacks.stanford.edu/file/druid:fg865kf5598/countering\\_prc\\_use\\_of\\_private\\_firms%20in\\_IO\\_gordian\\_knot\\_center\\_ver.pdf](https://stacks.stanford.edu/file/druid:fg865kf5598/countering_prc_use_of_private_firms%20in_IO_gordian_knot_center_ver.pdf).

<sup>41</sup> *Id.*

<sup>42</sup> *Id.* at 7.

<sup>43</sup> Office of the Director of National Intelligence, “Annual Threat Assessment of the U.S. Intelligence Community,” at 12 (Feb. 5, 2024) (“Annual Threat Assessment”) available at

<https://www.odni.gov/files/ODNI/documents/assessments/ATA-2024-Unclassified-Report.pdf>. National Intelligence Council, “Intelligence Community Assessment, Foreign Threats to the 2022 U.S. Elections,” ICA 2022-27259-A, at p. i (Dec. 23, 2022), available at

Assessment continued, “particularly on core sovereignty issues, such as Hong Kong, Taiwan, Tibet, and Xinjiang.”<sup>44</sup>

TikTok has announced that it has deployed “expert teams who focus entirely on detecting, investigating, and disrupting covert influence operations”<sup>45</sup> and now “label[s] the accounts and videos of media entities that we know to be subject to editorial control or influence by state institutions.”<sup>46</sup> But last-minute reforms—after years of criticism—do not negate the security threat posed by the PRC’s use of private firms such as TikTok to spread disinformation, conduct manipulation, and enable interference globally. And they certainly do not undermine Congress’s considered judgment that the threats posed by the PRC’s P-FIMI through TikTok warranted a legislative solution.

Regarding Wray’s second point, TikTok’s data collection is well-documented: “Despite TikTok vowing to curb the practice, it continues to access some of Apple users’ most sensitive data, which can include passwords, cryptocurrency wallet addresses, account-reset links, and personal messages.”<sup>47</sup> For example, last year, the

---

<https://www.dni.gov/files/ODNI/documents/assessments/NIC-Declassified-ICA-Foreign-Threats-to-the-2022-US-Elections-Dec2023.pdf>

<sup>44</sup> *Id.*

<sup>45</sup> TikTok, “Covert Influence Operations” (2024) available at <https://www.tiktok.com/transparency/en-us/countering-influence-operations/>

<sup>46</sup> TikTok, “Labelling State-Affiliated Media Entities” (2024), available at <https://www.tiktok.com/transparency/en-us/state-affiliated-media/>

<sup>47</sup> Dan Goodin, “TikTok and 32 other iOS Apps Still Snoop Your Sensitive Clipboard Data,” ARS TECHNICA (June 27, 2020), available at <https://arstechnica.com/gadgets/2020/06/tiktok-and-53-other-ios-apps-still-snoop-your-sensitive-clipboard-data/>.

*Wall Street Journal* reported that for “at least a year, some employees at TikTok were able to find what they described internally as a list of users who watch gay content on the popular app, a collection of information that sparked worker complaints.”<sup>48</sup> “Employees in China also had access to the data,” according to former employees, “and at times controlled the permissions for who could view the information.”<sup>49</sup> As the Respondent Government’s brief and U.S. media have reported, TikTok also collects data about the views of its American users on topics such as gun control and religion.<sup>50</sup> And TikTok agreed to pay a fine and alter its practices for violating the Children’s Online Privacy Protection Act by unlawfully collecting personal data of children.<sup>51</sup>

Nor is collection of information the only security risk posed by TikTok/ByteDance. The *New York Times* has reported that “TikTok user data [is] shared on” a company platform called “Lark,” which “is used every day by thousands

---

<sup>48</sup> Georgia Wells and Byron Tau, “TikTok Tracked Users Who Watched Gay Content, Prompting Employee Complaints,” *WALL ST. J.* (May 5, 2023), available at <https://www.wsj.com/articles/tiktok-tracked-users-who-watched-gay-content-prompting-employee-complaints-5966a5f5>.

<sup>49</sup> *Id.*

<sup>50</sup> See, e.g., Georgia Wells and Sadie Gurman, “TikTok Collected U.S. Users’ Views on Gun Control, Abortion and Religion, U.S. Says,” *WALL ST. J.* (July 27, 2024), available at [https://www.wsj.com/tech/tiktok-collected-u-s-users-views-on-gun-control-abortion-and-religion-u-s-says-4fcf19f6?st=hx3cqz2smfrso9s&reflink=article\\_email\\_share](https://www.wsj.com/tech/tiktok-collected-u-s-users-views-on-gun-control-abortion-and-religion-u-s-says-4fcf19f6?st=hx3cqz2smfrso9s&reflink=article_email_share).

<sup>51</sup> See Stipulated Order for Civil Penalties, Permanent Injunction, and Other Relief, *United States v. Music.ly*, No. 2:19-1439 (C.D. Cal.), available at [https://www.ftc.gov/system/files/documents/cases/musical.ly\\_proposed\\_order\\_ecf\\_2-27-19.pdf](https://www.ftc.gov/system/files/documents/cases/musical.ly_proposed_order_ecf_2-27-19.pdf).

According to the *Times*, user photos, countries of residence, internet protocol addresses, device and user IDs, and American driver's licenses were all accessible on the Lark platform, “as were some users’ potentially illegal content, such as child sexual abuse materials. In many cases, the information was available in Lark “groups” (chat rooms of employees) with thousands of members.”<sup>53</sup>

And beyond thousands of ByteDance employees in China viewing sensitive data, “a former employee of ByteDance, TikTok’s Beijing-based parent company, has outlined specific claims that the Chinese Communist Party accessed the data of TikTok users on a broad scale, and for political purposes.”<sup>54</sup>

**B. TikTok Enables the PRC to Interfere With U.S. Elections, Manipulate Information That Is Sensitive to China, and Conduct Psychological Warfare.**

That TikTok enables the PRC to interfere with U.S. elections, manipulate coverage of issues that are sensitive to Beijing, and wage psychological warfare has

---

<sup>52</sup> Sapna Maheshwari and Ryan Mac, “Driver’s Licenses, Addresses, Photos: Inside How TikTok Shares User Data,” *NEW YORK TIMES* (May 24, 2023), available at <https://www.nytimes.com/2023/05/24/technology/inside-how-tiktok-shares-user-data-lark.html>.

<sup>53</sup> *Id.*

<sup>54</sup> Brian Fung, “Analysis: There is Now Some Public Evidence that China Viewed TikTok Data,” *CNN BUSINESS* (June 8, 2023), available at <https://www.cnn.com/2023/06/08/tech/tiktok-data-china/index.html>; see also Alexandra Sternlicht, “Some Ex-TikTok Employees Say the Social Media Service Worked Closely With Its China-based Parent Despite Claims of Independence,” *FORTUNE* (Apr. 15, 2024), available at <https://fortune.com/2024/04/15/tiktok-china-data-sharing-bytedance-project-texas/>.

ample empirical support.

*Election interference.* The current Annual Threat Assessment stated point blank: “China is demonstrating a higher degree of sophistication in its influence activity, including experimenting with generative AI. *TikTok accounts run by a PRC propaganda arm reportedly targeted candidates from both political parties* during the U.S. midterm election cycle in 2022.”<sup>55</sup> Similarly, in 2022, the National Intelligence Council reported: “Key Judgment: The [Intelligence Community] assesses that China tacitly approved efforts to try to influence a handful of midterm races involving members of both US political parties. . . . We have high confidence in this assessment.”<sup>56</sup>

*Manipulating information sensitive to the PRC.* A new “Intelligence Report” by Rutgers University (the “Rutgers Study”) declared that “[t]he conclusions of our research are clear: Whether content is promoted or muted on TikTok appears to depend on whether it is aligned or opposed to the interests of the Chinese Government.”<sup>57</sup>

---

<sup>55</sup> *Supra* n. 44 (emphasis added).

<sup>56</sup> National Intelligence Council, “Intelligence Community Assessment, Foreign Threats to the 2022 U.S. Elections,” ICA 2022-27259-A, at i (Dec. 23, 2022), available at

<https://www.dni.gov/files/ODNI/documents/assessments/NIC-Declassified-ICA-Foreign-Threats-to-the-2022-US-Elections-Dec2023.pdf>.

<sup>57</sup> Network Contagion Research Institute (NCRI) and Miller Center on Policing and Community Resilience of Rutgers University, “A Tik-Tok-ing Timebomb: How TikTok's Global Platform Anomalies Align with the Chinese Communist Party's Geostrategic Objectives” (Dec. 2023), available at

[https://millercenter.rutgers.edu/wp-content/uploads/2024/01/A-Tik-Tok-ing-Timebomb\\_12.21.23.pdf](https://millercenter.rutgers.edu/wp-content/uploads/2024/01/A-Tik-Tok-ing-Timebomb_12.21.23.pdf).



More specifically: Using the same methods of analysis as did TikTok itself in defense to charges of antisemitism, the Rutgers Study compared relative hashtags used on TikTok and Instagram, TikTok's main competitor in social media.<sup>58</sup> It focused on six issues "directly sensitive" to the PRC: (1) the treatment of China's Uyghurs; (2) the killings in Beijing's Tiananmen Square in 1989; (3) China's annexation and administration of Tibet; (4) Hong Kong; (5) China's claim to Taiwan; (6) and China's claims on the South China Sea. It then added analyses of three additional areas, all relevant to the PRC's geopolitical interests: (1) the Ukraine-Russia war; (2) Kashmir independence; and (3) the Israel-Hamas war. The Study used, as a control group, topics concerning other political issues (not the ones that were "China-sensitive") and popular culture (such as pop music, video games, and sports). In the control group, hashtags in Instagram compared to TikTok were comparable, well within the ranges expected. For example, the video game Grand Theft Auto 6 was tagged just about evenly, 1:1, as was pop singer Shakira (0.9:1); Taylor Swift was more popular on Instagram (about 2:1) but still within the expected range, since the number of posts with pop culture hashtags on TikTok is approximately half that of Instagram.<sup>59</sup> The same was true for general political topics not specifically a worry of China's: the hashtag "Trump" was 2.2 times more prevalent on Instagram than TikTok, which, adjusted for the observed political biases in the users of the platform, was within the

---

<sup>58</sup> *Id.* at 3.

<sup>59</sup> *See id.* at 7.

expected range, *id.*; but so was the hashtag “BLM,” about 1.9:1. (The hashtag “Biden” was about even, 1:1.) Both were within the expected range given that hashtags related to politics are about twice as common on Instagram as on TikTok.

For China-sensitive topics, however, hashtags were wildly skewed. Hashtags with the word “Uyghur” were eleven times more common on Instagram as on TikTok. *Id.* at 9. “Tibet”-related hashtags were more than 37 times more common on Instagram. *Id.* at 10. “Hong Kong”-related hashtags were 181 times more common on Instagram. For hashtags related to Ukraine, the ratio was 8.5:1; for those supportive of Israel in its fight against Hamas, the ratio was 6.2:1; for those supportive of Kashmiri independence from India, a position considered in China’s interests, the ratio was, amazingly, less than one one-thousandth of one percent, Instagram to TikTok. It was, as the Study put it, “challenging to imagine that activity of such magnitude could occur on a platform organically, and without the knowledge and consent of the platform itself.”<sup>60</sup> The Study concluded: “[W]e assess a strong possibility that content on TikTok is either amplified or suppressed based on its alignment with the interests of the Chinese Government.”<sup>61</sup>

*Cognitive warfare.* Different authorities use different terms and definitions to describe “psychological warfare,” “information warfare,” or “cognitive combat.” But under any definition, security professionals concur on the basic tenet that the PRC’s

---

<sup>60</sup> *Id.* at 15.

<sup>61</sup> *Id.* at 16.

military and intelligence arms are using personal data, AI, and other technologies to develop psychological and biological weapons to undermine cognitively their adversaries.<sup>62</sup>

For example, a 2023 RAND Report found that

China views psychological warfare, centered on the manipulation of information to influence adversary decisionmaking and behavior, as one of several key components of modern warfare. . . . *The importance placed on psychological warfare is increasingly linked to Chinese military assessments that the cognitive domain will be a key domain of future warfare.* (emphasis added).<sup>63</sup>

China security analyst Craig Singleton at *Amicus* the Foundation for Defense of Democracies describes China’s billion-dollars-a-year campaign to build and deploy its cognitive warfare capacities.

On a basic level, Beijing’s discourse strategy seeks to alter global perceptions about Chinese autocracy and Western democracy . . . . In its most extreme form, called “cognitive domain warfare” (认知域作战) by China’s People’s Liberation Army, the CCP uses discourse power to influence individual and/or group behaviors to favor Beijing’s tactical or strategic objectives. This can be achieved by sowing social division, undermining faith in public institutions, introducing conflicting social

---

<sup>62</sup> See Bradley Bowman, ed., “Cognitive Combat China, Russia, and Iran’s Information War Against Americans,” FOUND. DEF. DEMOC., at 8-9 & nn. 9-18 (June 2024) (“FDD Monographs”), available at <https://www.fdd.org/wp-content/uploads/2024/06/fdd-monograph-cognitive-combat-china-russia-and-irans-information-war-against-americans.pdf>; see also Annual Threat Assessment, *supra* n. 40, at p. 12 (“**Beijing is expanding its global covert influence posture to better support the CCP’s goals.** The PRC aims to sow doubts about U.S. leadership, undermine democracy, and extend Beijing’s influence. . . . Beijing’s growing efforts to actively exploit perceived U.S. societal divisions using its online personas move it closer to Moscow’s playbook for influence operations.”) (bold in original).

<sup>63</sup> Nathan Beauchamp-Mustafaga, “Chinese Next-Generation Psychological Warfare,” RAND at iv-v (June 1, 2023) available at [https://www.rand.org/pubs/research\\_reports/RRA853-1.html](https://www.rand.org/pubs/research_reports/RRA853-1.html).

narratives, and radicalizing groups within a population.<sup>64</sup>

Duke Law School Professor Nita A. Farahany says that the “People’s Liberation army (PLA) is investing heavily in cognitive domain operations, including AI research in brain-inspired software, hardware and decision making.”<sup>65</sup> An integral part of this process is data-collection, AI, and FIMI-enabled by platforms such as TikTok: “Platforms like TikTok exemplify cognitive influence by shaping the beliefs and preferences of its vast user base while collecting data and developing psychogenic profiles of its users. TikTok’s algorithm has the power to mold public opinion and exploit user data to shape preferences, biases and beliefs.”<sup>66</sup> And while she endorses the Act banning TikTok, Prof. Farahany believes that it is not nearly enough to counter the growing threat posed by the PRC’s emerging cognitive warfare capacities:

While a TikTok ban may take out the first and fattest mole, it fails to contend with the wider shift to cognitive warfare as the sixth domain of military operations under way, which includes China’s influence campaigns on TikTok, a mass collection of personal and biometric data

---

<sup>64</sup> Craig Singleton, “China,” published in FDD Monographs, *supra* n.59 at 14 (June 202), available at

<https://www.fdd.org/wp-content/uploads/2024/06/fdd-monograph-cognitive-combat-china-russia-and-irans-information-war-against-americans.pdf>.

<sup>65</sup> See Nita Farahany, “TikTok is part of China’s cognitive warfare Campaign,” Opinion, GUARDIAN, (Mar. 25, 2023), available at

<https://www.theguardian.com/commentisfree/2023/mar/25/tiktok-china-cognitive-warfare-us-ban>; see also Bill Gerts, “Chinese ‘Brain Control’ Warfare Work Revealed,” WASH. TIMES, (Dec. 29, 2021) (reporting “three reports by the People’s Liberation Army [that] shed light on the depths of China’s brain warfare research and [that] show that it has been underway for several years.” One PLA report said that the “focus is to attack the enemy’s will to resist, not physical destruction,”), available at <https://www.washingtontimes.com/news/2021/dec/29/pla-brain-control-warfare-work-revealed/>.

<sup>66</sup> *Id.*

from American citizens and their race to *develop weapons that could one day directly assault or disable human minds*. We ignore this broader context at our peril. (emphasis added).<sup>67</sup>

In sum, TikTok is not merely a tool for Americans to enjoy “propaganda” from the PRC, as TikTok/ByteDance claims.<sup>68</sup> Rather, it is a tool that enables the PLA to obtain data (often covertly) and refine it with AI so that the PLA and the PRC’s intelligence services may fashion weapons to conduct psychological warfare against the United States and its allies in times of conflict. The First Amendment does not protect against that.

## **II. DIVESTITURE IS A REASONABLE REMEDY TO ADDRESS THE GRAVE NATIONAL SECURITY THREATS POSED BY TIKTOK AND BYTEDANCE.**

As the Government convincingly shows, Gov’t Br. at 18-57, the Act’s divestiture provisions are a reasonable means—at the very least—of addressing the serious threats to national security posed by TikTok and ByteDance.

*Deference to the Legislative and Executive Branches.* The Supreme Court has repeatedly instructed courts, in assessing the reasonableness of measures in the national security sphere, to tread relatively lightly. For example, *Holder v. Humanitarian Law Project* involved a challenge to a statute that criminalized providing “material support or resources” to “foreign terrorist organizations.”<sup>69</sup> The litigation there, like this case, concerned “sensitive and weighty interests of national

---

<sup>67</sup> *Id.*

<sup>68</sup> TikTok Brief, Doc. # 2060743, at 14, 50-58.

<sup>69</sup> 561 U.S. 1, 33 (2010).

security and foreign affairs.”<sup>70</sup> Thus, the Court held, the “evaluation of the facts” and “assessment[s]” by both the Executive and the Legislature are “entitled to deference.”<sup>71</sup> This is so because judges do not “begin the day with briefings that may describe new and serious threats to our Nation and its people.”<sup>72</sup> It is therefore “vital in this context not to substitute . . . [a court’s] evaluation of evidence for a reasonable evaluation by the Legislative Branch.”<sup>73</sup>

Similarly, in *Trump v. Hawaii*,<sup>74</sup> the Supreme Court upheld against constitutional challenge an executive order touching on core national security issues, and in doing so the Court relied in part on *Humanitarian Law Project* for the proposition that “when it comes to collecting evidence and drawing inferences” on questions of national security, “the lack of competence on the part of the courts is marked.”<sup>75</sup> This Court, too, has cited *Humanitarian Law Project* approvingly on this same point.<sup>76</sup>

*TikTok/ByteDance Intransigence.* Congress passed the Act after years of efforts by both the Executive and Legislative branches to reach a viable, amicable solution to

---

<sup>70</sup> *Id.* at 33-34.

<sup>71</sup> *Id.*

<sup>72</sup> *Id.*

<sup>73</sup> *Id.* at 34 (cleaned up; quoting *Boumediene v. Bush*, 553 U.S. 723, 797 (2008), and *Rostker v. Goldberg*, 453 U.S. 57, 68 (1981)).

<sup>74</sup> 585 U.S. 667 (2018).

<sup>75</sup> *Id.* at 704.

<sup>76</sup> *E.g.*, *China Telecom (Ams.) Corp. v. FCC*, 57 F.4th 256, 267 (D.C. Cir. 2022) (citing in turn *Olivares v. Transportation Sec. Admin.*, 819 F.3d 454, 466 (D.C. Cir. 2016), which quotes *Humanitarian Law Project*); *see also* Gov’t Br. at 66 (citing *Humanitarian Law Project*). *Ample Authority.*

stop TikTok/ByteDance’s abuses and respond to U.S. national security and privacy concerns. After years of knowingly failing to address the national security concerns of two Administrations and several Congresses, and after years of failing to end its objectionable practices on its own, TikTok/ByteDance now appears before this Court like some twenty-first century St. Augustine, who famously prayed, “Lord, give me chastity and continence, but not yet!” This Court cannot provide constitutional sanctuary for TikTok/ByteDance’s own actions. For the First Amendment does not enable TikTok/ByteDance to obtain, nor this Court to grant, last-minute absolution for years of Petitioners’ transgressions and abuses.

*Ample Authority.* Through the Act, Congress and the Executive are simply exercising powers that they have exercised before. For example, TikTok/ByteDance seek to cloak themselves in the First Amendment, but the Communications Act of 1934 generally requires majority American ownership of broadcast licenses (with certain exceptions for minority stakes), 47 U.S.C. § 310(b), and flatly prohibits ownership by a foreign government, *id.* § 310(a)—precisely what the Act does. And the very real national security concerns posed by TikTok/ByteDance, such as the potential blackmail of American citizens, are hardly novel: such concerns led the Committee on Foreign Investment in the United States to force a Chinese company to sell the LGBTQ+ dating app Grindr.<sup>77</sup>

---

<sup>77</sup> See, e.g., Yuan Yang and James Fontanella-Khan, “Grindr Is Being Sold by Chinese Owner After U.S. Raises National Security Concerns,” L.A. TIMES (Mar. 6, 2020) available at

*The Constitution Is Not a Suicide Pact.* Part I established that TikTok/ByteDance must comply with PRC laws providing extensive access to Chinese-owned companies' data, algorithms, and other information. The CAC can and did appoint one of four Board members to ByteDance, TikTok's parent. And PRC agencies and the CCP have infiltrated TikTok/ByteDance throughout their management and technical ranks, just as they do with other tech companies.

Part II.A established that TikTok collects or has collected data and personal information about its users, including children and users who view LGBTQ+ related videos. TikTok also shares user data with ByteDance in a chatroom called "Lark," available to thousands of employees. And ByteDance stores user information in the PRC. Part II.B established that TikTok has interfered in the 2022 midterm elections, manipulated information that is sensitive to the PRC and CCP, and has provided data, AI, and other technology that can assist the PLA and PRC intelligence services with their development of a psychological warfare capacity.

TikTok/ByteDance do not mention any of these actions or activities—not on their websites, not during Congressional testimony, not in the media, not in the Petition, and not in their brief. All of these activities raise national security concerns, and some pose actual threats to U.S. national security. None conceivably is protected by the First Amendment, but they are a legitimate basis for Congress to take legislative

---

<https://www.latimes.com/business/technology/story/2020-03-06/grindr-sold-by-chinese-owner-after-us-national-security-concerns>.



action to address these concerns and dangers.

Finally, even were the First Amendment somehow implicated by Congress's response to these threats, Congress passed the Act in the context of the PRC's threats to the independence of Taiwan; aggression toward U.S. allies in the South China Sea; challenges to freedom of navigation in contravention of the Law of the Sea Convention; aid to Russia in its war of aggression in Ukraine; spying in the U.S., including trade secrets and spy balloons; and election interference. The First Amendment surely does not prevent the Congress and the President from responding to these undeniable threats. As Justice Robert Jackson famously remarked 75 years ago, the Bill of Rights would become a "suicide pact" unless the courts of our nation "temper . . . doctrinaire logic with a little practical wisdom."<sup>78</sup> This Court should reject TikTok/ByteDance's arguments to the contrary.

## CONCLUSION

For the reasons set forth above, Amicus the Foundation for Defense of Democracies respectfully requests that this Court deny the Petitions for review.

---

<sup>78</sup> *Terminiello v. City of Chicago*, 337 U.S. 1, 37 (dissenting opinion).

Respectfully submitted,

/s/ \_\_\_\_\_

Peter C. Choharis  
Arnon D. Siegel  
THE CHOCHARIS LAW GROUP, PLLC  
1300 19th Street, NW, Suite 620  
Washington, DC 20036  
(202) 587-4478  
peter@chocharislaw.com

*Counsel for Amicus Curiae  
Foundation for Defense of Democracies*

**CERTIFICATE OF COMPLIANCE**

This brief complies with the type-volume limit of this Court's Rule 29(a)(5) and contains 5,975 words. This brief also complies with the typeface and type-style requirements of Federal Rule of Appellate Procedure 32(a)(5)-(6) because it was prepared using Word for Microsoft 365 in Times New Roman 14-point font, a proportionally spaced typeface.

/s/

\_\_\_\_\_  
Peter C. Choharis

**CERTIFICATE OF SERVICE**

I hereby certify that on this 2nd day of August, 2024, I caused true and correct copies of the foregoing Brief of *Amicus Curiae* Foundation for Defense of Democracies to be served via electronic mail upon all counsel of record, via the Court's ECF system.

/s/  
Peter C. Choharis